Auditdienst Rijk
Ministerie van Financiën

Rapportage onderzoek interceptiefaciliteit
Kenmerk ADR/2014/1470

Versie 1.0

Datum	9 december 2014
Status	Definitief

Colofon

Titel	Rapportage onderzoek interceptiefaciliteit
Auteur(s)	Auditdienst Rijk
Bijlage(n)	2

Inlichtingen

Auditdienst Rijk
T 070-3427700
F 070-3427701

Inhoud

1 Algemeen

1.1 Inleiding

Naar aanleiding van de storing in de interceptiefaciliteit van 20 september 2012 heeft de minister van Veiligheid en Justitie op 17 december 2013 een brief aan de Tweede Kamer gestuurd waarin een aantal toezeggingen is gedaan ten aanzien van de interceptiefaciliteit van de Nationale Politie. Eén van deze toezeggingen betreft het door de Auditdienst Rijk (ADR) uitvoeren van een onderzoek naar de huidige interceptiefaciliteit.

1.2 Context

Vanwege de complexiteit van interceptie in combinatie met de snelle technologische ontwikkelingen op het terrein van telecommunicatie is in 2000 op initiatief van de ministers van Justitie en Binnenlandse Zaken en Koninkrijksrelaties (BZK) de herstructurering van de interceptiefaciliteit in gang gezet met de ambitie om te komen tot één centrale organisatie voor het tappen (Tweede Kamer, 2002-2003, 29200 VII nr. 39). De afdeling Interceptie & Sensing (I&S) van de Landelijke Eenheid (voorheen Korps Landelijke Politiediensten) verzorgt op dit moment de interceptie voor de Nationale Politie, de Rijksrecherche, de bijzondere opsporingsdiensten en de Koninklijke Marechaussee. Op 1 september 2011 is de huidige interceptiefaciliteit in gebruik genomen. Zowel de interceptie zelf als ook de technische infrastructuur die hiervoor nodig is, is complex. Hierdoor is de kans op storingen hoog.

1.3 Opdracht

Dit onderzoek geeft antwoord op de vragen die de ADR zijn aangereikt als onderdeel van de nota "Toezeggingen op tapdossier" van DGPol, d.d. 15 april 2014. Het onderzoek is bedoeld om tegemoet te komen aan de toezegging van de Minister aan de Tweede Kamer d.d. 17 december 2013 om de ADR een onderzoek te laten uitvoeren naar de interceptiefaciliteit en de Tweede Kamer over de uitkomsten hiervan te informeren.

De vier onderwerpen van het onderzoek zijn:
- de storing van 20 september 2012;
- de maatregelen die zijn genomen vanaf december 2013;
- de opvolging van de aanbevelingen uit eerdere reguliere audits;
- de registraties en procedures bij storingen.

1.4 Afbakening

Het doel van het onderzoek is door de Minister in de brief van 17 december 2013 aangegeven. In de opdracht van DGPol aan de ADR is het doel van het onderzoek nader uitgewerkt in de vier hiervoor genoemde onderwerpen met per onderwerp een aantal onderzoeksvragen.

Het onderzoek heeft een tweeledig karakter. Het eerste deel betreft een feitenonderzoek naar de storing op 20 september 2012, de naleving van de procedures en de opvolging van de aanbevelingen uit eerdere reguliere audits. Het tweede deel van het onderzoek betreft de maatregelen die getroffen zijn na december 2013.

De opdracht aan de ADR valt onder richtlijn 4401 van het NOREA[1)], gericht op specifiek overeengekomen werkzaamheden met betrekking tot informatietechnologie en leidt tot een rapport van feitelijke bevindingen. Dit betekent dat geen conclusies worden geformuleerd met betrekking tot de onderzoeksvragen. Tevens houdt dit in dat indien aanvullende werkzaamheden, een controle- of beoordelingsopdracht zou zijn uitgevoerd, wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.
Dit onderzoek betreft geen forensisch en ook geen persoonsgericht onderzoek. De bewijskracht voor de bevindingen is afhankelijk van de bron, dat in paragraaf 1.6 nader wordt toegelicht.
Voorts merken wij op dat de interceptiefaciliteiten van I&S niet alleen tapdata voor spraak veilig stelt, maar ook sms-berichten, internetverkeer e.d. Het onderzoek richt zich op dat deel van het tapsysteem dat betrekking heeft op spraak.

1.5 Werkzaamheden

Voor de beantwoording van de onderzoeksvragen hebben wij de volgende werkzaamheden uitgevoerd:

- Het bestuderen van relevante documenten over het tapincident.
- Het kennis nemen van documentatie van het tapsysteem, de specifieke storing op 20 september 2012 die aanleiding is van het incident en het oplossen van de betreffende storing.
- Het houden van interviews met medewerkers van I&S en de leverancier van het tapsysteem en het opvragen van aanvullende documentatie.
- Het afstemmen van de interviewverslagen met de geïnterviewden.
- Het analyseren van loggingen en data uit het systemen.
- Het analyseren en evalueren van de bevindingen ter beantwoording van de onderzoeksvragen.
- Het afstemmen van de feitelijke bevindingen met betrokkenen binnen de Nationale Politie.
- Het afstemmen van de resultaten met de opdrachtgever.

1.6 Bronnen van onderzoek

De aantoonbaarheid van de feiten ten aanzien van de storing op 20 september 2012 moet komen uit interviews, procedurele vastleggingen van storingen en beheerwerkzaamheden en tenslotte uit de logging van de systemen. Hierbij moet rekening worden gehouden dat de waarde van de interviews over een storing die twee jaar geleden heeft plaatsgevonden, beperkt is. Eigen (directe en daardoor geobjectiveerde) waarnemingen door de auditors zelf over de toedracht van de storing zijn niet mogelijk, aangezien deze in het verleden heeft plaatsgevonden.

De aard van de bron is bepalend voor de informatiewaarde voor ons onderzoek. Hierdoor vertoont de informatiewaarde de volgende afnemende valideerbaarheid van de verkregen informatie.
Als eerste de data uit systemen en de loggingen; vervolgens de documentatie over tapsysteem, parameterinstellingen en procedures; de procedurele vastleggingen in de interne registratiesystemen, en als laatste de interviews met betrokkenen. Hierbij dient te worden benadrukt dat de waarde die ontleend kan worden aan een interview (twee jaar na het incident) niet gelijk is aan bewijs verkregen uit registraties en loggingen.
De analyse van de loggingen is gedaan op de bestanden die door I&S zijn aangeleverd. De bestanden zijn door de leverancier in opdracht van I&S in 2013 veilig gesteld. Wij hebben niet zelf de data en de loggingen uit de systemen onttrokken.

1) Nederlandse Orde van Register EDP-Auditors

1.7 Leeswijzer

De doelgroep van de rapportage is de opdrachtgever de minister van Veiligheid en Justitie en de gedelegeerd opdrachtgever DGPol. De opdrachtgever is verantwoordelijk voor afstemming van deze rapportage met de Nationale Politie en voor de verspreiding van de rapportage naar derden, waaronder de Nationale Politie en de Tweede Kamer.

Het resultaat van deze opdracht is een rapportage met de beantwoording van de onderzoeksvragen op basis van de feitelijke bevindingen. Hierbij wordt rekening gehouden met de beperkingen die inherent zijn aan de bronnen van onderzoek.
In dit onderzoeksrapport wordt geen oordeel gegeven over de kwaliteit van de interceptiefaciliteit.

In hoofdstuk 2 is de samenvatting opgenomen, waarna in hoofdstuk 3 antwoord wordt gegeven op de onderzoeksvragen, zoals die door de opdrachtgever voor het onderzoek zijn aangegeven. In de bijlagen zijn een begrippenlijst en de tijdlijn van de gebeurtenissen rond de storing in 2012 en het hierdoor ontstane incident in 2013 opgenomen.

2 Samenvatting

Naar aanleiding van de storing in het tapsysteem op 20 september 2012 heeft de minister van Veiligheid en Justitie op 17 december 2013 een brief aan de Tweede Kamer gestuurd waarin een aantal toezeggingen is gedaan ten aanzien van de interceptiefaciliteit van de Nationale Politie. Eén van deze toezeggingen betreft een door de Auditdienst Rijk (ADR) uit te voeren onderzoek naar de huidige interceptiefaciliteit. De Minister heeft toegezegd de Tweede Kamer na de zomer 2014 te informeren over de uitkomsten van dit onderzoek.

Het Directoraat-Generaal Politie heeft de ADR op 15 april 2014 de onderzoeksvragen aangereikt. Het onderzoek is uitgevoerd in de periode juni tot en met september 2014.

Bij dit onderzoek zijn de volgende omstandigheden relevant:
- het storingsincident heeft circa twee jaar geleden plaatsgevonden;
- wij ons moeten baseren op kennis die twee jaar terug gaat in de tijd;
- niet alle loggingen en toentertijd bestaande systeeminstellingen zijn bewaard gebleven;
- de storing is niet vastgelegd in de incidentenregistratie van Interceptie & Sensing (I&S) waardoor dit aanknopingspunt voor het onderzoek niet aanwezig is.

Dit rapport van bevindingen is het resultaat van ons onderzoek en geeft antwoord op de aan ons aangereikte vragen. De beantwoording van de onderzoeksvragen is gerubriceerd naar de aan ons aangereikte vier onderwerpen.

De storing op 20 september 2012
Op 20 september 2012 heeft er een storing plaatsgevonden in de tapsysteem van de Landelijke Eenheid van de Nationale Politie. De storing had alleen betrekking op het tappen van spraak. Andere vormen van tappen, zoals internettaps, zijn niet door deze storing geraakt. De storing begon om 13:14 en eindigde om 14:04. In dit tijdsbestek van vijftig minuten zijn geen gesprekken en verkeersgegevens vastgelegd in het tapsysteem. Dit blijkt onder andere uit de loggegevens van het tapsysteem van die bewuste dag. Wij hebben geen sporen aangetroffen dat er sprake is van wissen van gesprekken die gevoerd zijn op 20 september 2012.
Uit interviews en procesregistraties komt naar voren dat een defect geraakte voeding, in combinatie met firmware die niet up to date was, de oorzaak van de storing kan zijn geweest. De exacte oorzaak van de storing hebben wij, op basis van de beschikbare bronnen, niet kunnen achterhalen.
Essentiële onderdelen van het systeem, zoals voedingen, zijn dubbel uitgevoerd. De in het tapsysteem aanwezige voorzieningen zijn erop gericht om dergelijke storingen te voorkomen.

Op 20 september 2012 waren er ongeveer 1800 taps in bedrijf. Wij schatten in dat door de storing ongeveer 1250 getapte gesprekken niet zijn vastgelegd.
De storing is dezelfde dag gesignaleerd, verholpen en geregistreerd door een technisch beheerder van de leverancier van het tapsysteem, die onderdeel uitmaakt van het beheer van het tapsysteem door I&S. In deze registratie is aangegeven dat er sprake is van een storing met dataverlies. De leverancier heeft in oktober 2012 één van de twee voedingen en de systeemsoftware van deze opslagcomponent vernieuwd.
De storing is niet geregistreerd door I&S. Hierdoor is het incidentenproces niet opgestart, geen proces-verbaal opgesteld en de opsporingsteams zijn niet geïnformeerd over deze storing. Wij hebben geen eenduidige reden aangetroffen

waaruit blijkt waarom dit incidentenproces niet heeft gefunctioneerd. Hier spelen twee factoren een rol:

1. De leverancier heeft ons informatie aangereikt waaruit blijkt dat zij de storing van 20 september 2012 niet volgens de geldende werkwijze heeft doorgegeven aan I&S.
2. I&S beschikt over een monitoringsysteem die afwijkingen in het functioneren van het tapsysteem signaleert en berichten kan uitsturen. Het is niet duidelijk geworden of dit monitoringsysteem van de bewuste storing berichten heeft verstuurd en zo ja of I&S deze heeft ontvangen.

Op 9 september 2013 is tijdens een regiezitting door de verdediging gesteld dat een tapgesprek ontbreekt in het strafdossier. Op 19 september 2013 wordt duidelijk dat op 20 september 2012 een storing heeft plaatsgevonden in de tapfaciliteit van de politie. Op het moment dat de volle omvang van de storing duidelijk werd, was de wettelijke retentietermijn van 1 jaar voor het opvragen van verkeersgegevens van 20 september 2012 verstreken.
Op verzoek van I&S rapporteert de leverancier na onderzoek op 23 september 2013 over de storing. I&S heeft op 5 december 2013 een proces-verbaal opgesteld ten behoeve van alle opsporingsonderzoeken die actieve telefoontaps hadden op 20 september 2012. Hiermee zijn alle onderzoeksteams geïnformeerd.

Maatregelen genomen vanaf december 2013
In de brief aan de Tweede Kamer heeft de Minister de maatregelen die de korpschef heeft getroffen opgenomen. Hieronder geven wij de stand van zaken van deze maatregelen aan.

1. *Het opheffen van tekortkomingen in het incidentenproces van I&S*
   Per 11 juni 2014 is een nieuwe procesbeschrijving 'Incidentmanagement I&S' beschikbaar gekomen met de status definitief. In aanloop op de nieuwe procesbeschrijving zijn de medewerkers en de leidinggevenden van I&S sinds december 2013 geïnstrueerd over een adequate behandeling van incidenten en is de werkwijze aangepast. Thans wordt gewerkt aan een volledige uitwerking en implementatie van het nieuwe proces.

2. *Het treffen van een technische noodvoorziening ter voorkoming van mislukte interceptie van telefoongesprekken*
   Samengevat geeft de korpsleiding aan dat uit analyse van de storing is gebleken dat het uitbreiden van de noodvoorziening geen oplossing biedt voor storingen zoals die op 20 september 2012 is opgetreden en leiden tot het mislukken van interceptie. Het huidige tapsysteem is ontworpen om zoveel mogelijk dataverlies te voorkomen, waarin de kritische componenten dubbel zijn uitgevoerd. Het rekencentrum voldoet aan de wereldwijde standaarden voor dit soort centra en is uitwijk voorzien in de vorm van het testsysteem. De korpsleiding komt aan de hand daarvan tot de conclusie dat extra investeren in technische (nood)voorzieningen afgewogen moeten worden ten opzichte van de huidige situatie. Het is dan ook bedrijfsmatig verstandig is om de lessen uit dit incident te vertalen in de eisen aan het nieuwe systeem en voor de bestaande situatie in te zetten op aanscherping van procedures en werkwijzen. Dit laatste is reeds in werking gesteld.
   De bestaande uitwijkvoorziening in de vorm van het testsysteem op een andere locatie heeft een lagere capaciteit als het reguliere systeem, daardoor kan niet volledig worden uitgeweken.

3. *Het door experts laten bezien in hoeverre er mogelijkheden zijn om de technische beschikbaarheid van het tapsysteem verder te verhogen*
   Samengevat geeft de korpsleiding aan dat de technische beschikbaarheid van het tapsysteem 99,5% is zonder dataverlies. Door experts vanuit de Landelijke Eenheid (LE) en de Informatievoorzieningorganisatie (IV) is besproken welke mogelijkheden er zijn ter verbetering van de technische beschikbaarheid.

Voorts geeft zij aan dat aangezien de voorbereidingen gestart zijn voor een aanbesteding voor de vervanging van het tapsysteem, de experts tot de conclusie zijn gekomen dat het beter is daarin te investeren dan tegen hoge kosten te proberen de laatste 0,5% in het huidige systeem te reduceren.

4. *Het overdragen van het beheer van het tapsysteem van I&S aan de dienst Informatievoorziening wordt versneld voorbereid*
   Samengevat geeft de korpsleiding aan dat de voorbereiding is versneld door het in kaart brengen van de risico's verbonden aan de overdracht. Een versnelde overdracht van het huidige tapsysteem aan de dienst ICT werkt risicoverhogend, omdat de complexiteit van het systeem hoog is en de benodigde expertise schaars. Daarnaast speelt dat de overdracht een beroep doet op (schaarse) ICT capaciteit, hetgeen consequenties heeft voor binnen het aanvalsprogramma ICT geprioriteerde lopende of geplande projecten. De geformuleerde eisen aan de geplande vernieuwing in 2016 zullen resulteren in een reductie van de afhankelijkheden tussen de diverse componenten. De korpsleiding concludeert dat op grond hiervan het logisch is de overdracht uit te voeren in samenhang met de implementatie en ingebruikname van het nieuwe systeem.
   Over de relatie van deze maatregel met de hoge beschikbaarheid van het tapsysteem kunnen wij geen uitspraak doen.

5. *Het spoedig doen van een voorstel voor een nieuw stelsel voor informatiebeveiliging van de politie*
   Samengevat geeft de korpsleiding aan dat de politie al geruime tijd bezig is haar stelsel informatiebeveiliging te vernieuwen. Hierbij maakt zij een omslag naar een risico gebaseerd stelsel. Op basis van haar verzoek aan DGPol is deze laatste acties gestart voor het herzien van het verouderde stelsel. In afstemming met DGPol handelt de korpsleiding thans naar het nieuwe stelsel, vooruitlopende op de herziening.
   Een adequaat stelsel voor informatiebeveiliging is randvoorwaardelijk voor een hoge beschikbaarheid. Door gerichte maatregelen kan het bijdragen aan de hoge beschikbaarheid.

Opvolging aanbevelingen vanuit eerdere reguliere audits
In 2007 en 2011 zijn reguliere audits uitgevoerd naar de interceptiefaciliteit. Hier zijn aanbevelingen uit voortgekomen, welke deels zijn gerealiseerd. Drie belangrijke aanbevelingen zijn niet gerealiseerd, namelijk:
1. het evalueren en actualiseren van de "Normstelling Inrichting Interceptiefaciliteit" uit 2004;
2. het opstellen van een kalender met kritieke beheershandelingen, controle op deze beheershandelingen en periodieke interne audits;
3. het treffen van maatregelen rondom leverancierstoegang tot het interceptiesysteem voor spraak.

Het evalueren van de normstelling is een verantwoordelijkheid van de beleidsdirectie DGPol. I&S is voornemens de laatste twee aanbevelingen mee te nemen in het totale pakket van verbeteringen van de interceptiefaciliteit.

Registratie en procedures bij storingen
In juni 2014 is een vernieuwde procesbeschrijving incidentenmanagement I&S formeel vastgesteld. Deze is nog niet uitgewerkt in werkinstructies en geïmplementeerd. In aanloop hierop zijn de medewerkers en de leidinggevenden van I&S sinds december 2013 geïnstrueerd over een adequate behandeling van incidenten en is de werkwijze aangepast. Thans wordt gewerkt aan een volledige uitwerking en implementatie van het nieuwe proces.
In de nieuwe procesbeschrijving zijn de rollen duidelijk aangegeven, bijvoorbeeld dat de voortgang en afhandeling van meldingen wordt bewaakt door de incidentcoördinator. De wijze waarop de registratie van een technische storing plaatsvindt, is opgenomen in deze procesbeschrijving. Hierin ontbreekt overigens de

wijze waarop meldingen van de technisch beheerder van de leverancier van het tapsysteem worden opgenomen in de incidentenregistratie van I&S.
Dit betekent dat de werkwijze die bestond ten tijde van de storing tot begin 2014 niet principieel is gewijzigd, maar wel aangescherpt. De aanscherping betreft met name het verplicht opmaken van een proces-verbaal ingeval van dataverlies.

Om een hoge beschikbaarheid van het tapsysteem te borgen heeft I&S technische en procedurele maatregelen getroffen. Met name de procedurele maatregelen behoeven aanvulling, zoals uitwijkscenario en periodiek testen van de uitwijk.

Over de beschikbaarstelling van de tapfaciliteit met de daarbij behorende serviceniveaus van I&S aan de opsporingsteams hebben wij geen concrete afspraken aangetroffen. De dienstverlening van I&S aan de opsporingsteams is 7x24 uur. Hierbij is geen indicatie aangegeven over de hersteltijd in geval van een storing. Ook de beschikbaarheid op jaarbasis in percentage is niet aangegeven.

Met de leveranciers van hard- en software, de IV-organisatie en de Telecom aanbieders zijn afspraken gemaakt over de kwaliteit van de diensten, de beschikbaarheid van de dienstverlening, de wijze van het melden van (ver)storingen en de tijdigheid van het oplossen ervan.

3 Beantwoording onderzoeksvragen

3.1 Onderzoeksomgeving

Voordat ingegaan wordt op de beantwoording van de deelvragen, wordt eerst een beeld geschetst van de algemene situatie van I&S zoals dit bij de onderzoekers is overgekomen. Het is belangrijk om hiervan kennis te nemen, aangezien dit verklaart waarom de processen op een dergelijke wijze worden uitgevoerd.

In 2011 heeft de Landelijke Eenheid (voorheen Korps Landelijke Politie Diensten) de interceptiefaciliteit vernieuwd en is het beheer hiervan bij de afdeling I&S belegd. Hoewel de hardware van de interceptiefaciliteit is ondergebracht in het rekencentrum van de dienst ICT (onderdeel van de IV-organisatie, voorheen vtsPN) van de politie, heeft de dienst ICT geen bemoeienis met het onderhoud en het beheer ervan.
De interceptiefaciliteit betreft een complexe ICT-infrastructuur (hardware) met evenzo complexe software. Daarbij komt dat door de technologische ontwikkelingen op het gebied van telecommunicatie de interceptiefaciliteit voortdurend aan veranderingen onderhevig is. Om een dergelijk systeem te beheren zijn gespecialiseerde beheerders en onderhoudstechnici nodig. In een deel van deze behoefte wordt voorzien door met de leveranciers van de tapsystemen onderhoudscontracten af te sluiten. De rest van het beheer wordt ingevuld door Technisch Support (TS) van I&S zelf.

In de volgende paragrafen worden de onderzoeksvragen beantwoord zoals die door de opdrachtgever zijn meegegeven. Paragraaf 3.2 gaat in op de storing zelf, waarbij onder meer de oorzaak en de gevolgen worden toegelicht. In paragraaf 3.3 wordt ingegaan op de maatregelen die naar aanleiding van het incident zijn genomen. Hierbij worden ook ontwikkelingen weergegeven die in zijn algemeenheid bijdragen aan verbeteringen van het interceptieproces en de –faciliteit.

In paragraaf 3.2 wordt eerst het antwoord gegeven op de vraag, waarna deze wordt toegelicht aan de hand van de bevindingen uit de bronnen die in volgorde van aflopende informatiewaarde zijn weergegeven.

3.2 De storing van 20 september 2012

3.2.1 Wat was de exacte (technische) oorzaak van de storing?

De exacte oorzaak van de storing is op basis van de aanwezige geautomatiseerde vastleggingen niet meer vast te stellen. De storing is niet in de incidentenregistratie van I&S vastgelegd. Er is door I&S geen onderzoek uitgevoerd naar de oorzaak van de storing, direct nadat de storing op 20 september 2012 heeft plaatsgevonden. Hierdoor missen wij deze informatie voor het onderzoek.
Uit een e-mailbericht van de leverancier van 10 oktober 2012 blijkt dat het disfunctioneren (haperen) van een voeding in de opslagcomponent mogelijk instabiliteit heeft veroorzaakt. Daarbij komt dat de systeemsoftware (firmware) van de opslagcomponent niet up-to-date was. Op het moment van de instabiliteit wordt het onderlinge contact tussen de enkele onderdelen van het tapsysteem verbroken. Hierdoor wordt de binnenkomende tapdata voor spraak niet meer opgeslagen en gaat verloren.

Uit de in 2013 veilig gestelde logbestanden die wij door I&S aangereikt hebben gekregen, blijkt dat op 20 september 2012 gedurende 50 minuten de verbinding tussen de verwerkingscomponent en de opslagcomponent van het tapsysteem verbroken is geweest. In de loggingen van deze component is tot op de seconde nauwkeurig zichtbaar dat de opslagcomponent om 13:14 uitvalt en om 14:04 weer

actief wordt. Eén foutmelding geeft letterlijk aan dat de opslagcomponent is uitgevallen. Gedurende deze 50 minuten storing worden geen verkeersgegevens en gesprekken opgeslagen.
De in het tapsysteem aanwezige voorzieningen hadden deze uitval moeten voorkomen. Deze voorziening heeft niet gewerkt door mogelijk het niet goed functioneren van de firmware.

De mogelijkheid dat tapdata opzettelijk is gewist, hebben we onderzocht aan de hand van de registratie van tapgesprekken in de zaak Van Rey. Wij hebben vastgesteld dat de doorlopende nummering van de opgeslagen tapgesprekken niet is onderbroken. De audittrail geeft geen aanwijzingen en dat er sprake is van wissen van gesprekken die zijn gevoerd op 20 september 2012.

3.2.2 *Indien de storing, conform het ambtsbericht, te wijten is aan de voeding: hoe kan het dat daardoor het gehele systeem is uitgevallen, terwijl het twee voedingen kent en bij het uitvallen van één voeding onverminderd operationeel zou moeten blijven?*

Op 20 september 2012 is, ten tijde van de storing, niet het gehele tapsysteem uitgevallen. De verwerkingscomponent en de bijbehorende opslagcomponent van de binnenkomende tapdata voor spraak hebben niet gefunctioneerd. De andere tapfaciliteiten, zoals sms- en internetverkeer zijn onverminderd operationeel gebleven.

Een van functionele eisen van het tapsysteem is dat essentiële onderdelen dubbel zijn uitgevoerd. Hiermee wordt beoogd dat bij uitval van deze onderdelen het tapsysteem onverminderd operationeel blijft. Dit betekent dat de meeste systeemcomponenten zijn voorzien van dubbele voedingen.
Het tapsysteem voor spraak is zo ontworpen dat wanneer één verwerkingscomponent van het tapsysteem de verbinding met de opslagcomponent verliest de tweede verwerkingscomponent het overneemt. Omdat beide verwerkingscomponenten offline waren, was er geen actieve verwerkingscomponent om de binnenkomende gesprekken te verwerken. De binnenkomende verkeersgegevens en gesprekken werden niet meer opgeslagen en raakten verloren.

Het disfunctioneren van de voeding en het daadwerkelijk defect raken daarvan hebben wij niet uit de loggingen kunnen vaststellen. In de rapportage van 23 september 2013, van de technisch beheerder van de leverancier over de storing van 20 september 2012, wordt het falen van de voeding als oorzaak aangegeven.
Wij hebben in de logging vastgesteld dat een instabiliteit is opgetreden in de vorm van het stoppen van services van de verwerkingscomponent. Ook hebben wij in de logging vastgesteld dat de verbinding met de opslagcomponent in die tijd is verbroken.

3.2.3 *Wat waren de gevolgen van de storing in brede zin en voor de lopende taps in het bijzonder?*

Uit het onderzoek komt naar voren dat door de storing op 20 september 2012 tussen 13:14 en 14:04 uur dataverlies is opgetreden en dat voor alle actieve taps voor spraak (ongeveer 1800) geen verkeersgegevens en gesprekken zijn opgeslagen. Doordat de storing door I&S niet is opgemerkt en ook niet door de technisch beheerder van de leverancier aan I&S is gemeld, is het incidentenproces van I&S niet gestart en derhalve niet doorlopen. Het gevolg hiervan is dat geen analyse of onderzoek door I&S heeft plaatsgevonden waardoor ook niet kon worden onderkend dat sprake is geweest van een storing met dataverlies. Daarom zijn de Regionale Interceptie Coördinatoren (RIC-ers) op dat moment niet geïnformeerd, en is ook geen proces-verbaal opgesteld over de storing.
Uit de incidentenregistratie van de leverancier van het tapsysteem blijkt dat de storing daar wel is geregistreerd. Wij hebben aanwijzingen dat de leverancier deze

storing niet conform de procedure heeft gemeld aan I&S. Na het bekend worden van het incident in september 2013 heeft de leverancier op verzoek van I&S onderzoek gedaan en op 23 september 2013 een rapportage over de storing opgeleverd.

In de interviews geeft I&S aan niet op de hoogte te zijn geweest van de storing op 20 september 2012 en hiermee voor het eerst te zijn geconfronteerd door de zaak van Van Rey in september 2013. Op grond hiervan heeft I&S onderzoek uitgevoerd naar het ontbreken van tapgesprekken. Op basis van dat onderzoek is bij I&S duidelijk geworden dat op 20 september 2012 een storing is opgetreden met dataverlies voor alle op dat moment actieve taps voor spraak.

3.2.4 *Op welke manier en door wie is de storing gesignaleerd en doorgegeven aan de eenheden?*

De storing van 20 september 2012 is op dezelfde dag gesignaleerd, opgelost en intern geregistreerd door de technisch beheerder van de leverancier van het tapsysteem, die onderdeel uitmaakt van het beheer van het tapsysteem door I&S. Er zijn geen aanwijzingen dat de leverancier conform de gangbare werkwijze I&S schriftelijk heeft geïnformeerd over de storing met mogelijk dataverlies. I&S heeft daarom op dat moment de eenheden niet kunnen informeren over de storing.
Op 9 september 2013 is tijdens een regiezitting door de verdediging gesteld dat een tapgesprek ontbreekt in het strafdossier. Door de Rijksrecherche en I&S is in september 2013 onderzoek uitgevoerd naar de oorzaak en het gevolg van de storing op 20 september 2012. Naar aanleiding van de uitkomsten van dit onderzoek heeft I&S op 5 december 2013 een proces-verbaal opgesteld voor alle op 20 september 2012 actieve taps voor spraak en dit is vervolgens per e-mail meegedeeld aan de eenheden.

Wij hebben in de incidentenregistratie van I&S geen melding over de storing van 20 september 2012 aangetroffen. Daarbij kan geen van de geïnterviewde functionarissen van I&S zich herinneren een e-mailbericht van het technisch beheer van de leverancier over de storing te hebben ontvangen. Ook het onderzoek van de centrale mailbox van Technisch Support, waarin alle e-mailberichten binnen komen, heeft geen resultaten opgeleverd. De leverancier van het tapsysteem heeft naderhand bevestigd dat geen e-mailbericht aan I&S is te achterhalen over de storing van 20 september 2012.

I&S maakt gebruikt van een health-monitor. De functie van deze health-monitor is om de status van hardware en software componenten en hun onderlinge samenhang bij voortduring te meten en afwijkingen te signaleren. De health-monitor beschikt over de functionaliteit om detectieve signalen te versturen door bijvoorbeeld sms-berichten. Door parametrisering van de health-monitor wordt aangegeven voor welke kritieke situaties sms-berichten worden verzonden. Wij hebben onvoldoende informatie kunnen krijgen om vast te stellen dat dit heeft plaatsgevonden. Conform de toen geldende instellingen werden de sms-berichten van de health monitor twee weken bewaard. Deze zijn derhalve niet beschikbaar voor analyse.
Geen van de geïnterviewde personen van I&S kan zich herinneren een sms-bericht te hebben ontvangen van de health-monitor over de storing van 20 september 2012. Wij merken op dat het wel of niet ontvangen van sms-berichten wordt bepaald door de piketdiensten.

3.2.5 *Op welke manier en door wie is opvolging gegeven aan (het verhelpen van) de storing?*

Op 20 september 2012, de dag van de storing, is door de technisch beheerder van de leverancier de storing gesignaleerd en door middel van het handmatig herstarten van de services is de storing opgelost. Wij hebben niet kunnen vaststellen dat I&S over deze storing door de technisch beheerder van de leverancier is geïnformeerd.

Op 11 oktober 2012 heeft de leverancier van het tapsysteem één van de twee voedingen van de opslagcomponent vervangen. Op 15 oktober 2012 is de systeemsoftware (firmware) vernieuwd.

Wij hebben niet de beschikking gekregen over logging van de bovengenoemde beheerhandelingen. Uit andere informatiebronnen blijkt dat een voeding is vervangen.

Vanwege het dataverlies dat gepaard gaat met een handmatige herstart, is hiervoor toestemming nodig van de leiding van Technisch Support. In de incidentenregistratie van I&S hebben wij geen registratie aangetroffen waaruit blijkt dat op 20 september 2012 toestemming is gegeven voor een herstart van de services. Wij hebben noch uit interviews, noch uit de door ons ontvangen documenten, kunnen achterhalen of en zo ja door wie hiervoor toestemming is gegeven. De gangbare werkwijze die de technische beheerder van de leverancier aangeeft, is dat in urgente gevallen eerst mondeling toestemming wordt gegeven, waarna deze naderhand schriftelijk wordt bevestigd. Een dergelijke schriftelijke bevestiging hebben wij niet aangetroffen.

Door de leverancier wordt per e-mailbericht op 10 oktober 2012 aan Technisch Support van I&S gemeld dat de voeding van de opslagcomponent defect is en dat dit de mogelijke oorzaak is van de instabiliteit. Ook geeft hij aan dat de firmware van de opslagcomponent moet worden vernieuwd. Een voeding is op 11 oktober 2012 vervangen en op 15 oktober is de firmware vernieuwd. Van beide activiteiten heeft geen registratie plaatsgevonden in de incidentenregistratiesysteem van I&S.

Dat de vervanging van een voeding daadwerkelijk heeft plaatsgevonden leiden wij af door de bezoekersregistratie van het Rekencentrum te confronteren met de logging van de cyberkey waarmede toegang tot de server rack's wordt verkregen. Het vervangen van een voeding door een zwaarder type hebben wij niet kunnen vaststellen.

3.2.6 *Op welke manier en door wie is een proces-verbaal opgesteld over de storing ten behoeve van opsporingsonderzoeken in de periode tot september 2013?*

Voor het opstellen van een proces-verbaal gold vanaf 2008 tot juni 2014 een procedure die I&S heeft opgesteld. Deze procedure[1)], waaronder analyse of onderzoek om vast te stellen dat er mogelijk sprake is van dataverlies en het opmaken van het proces-verbaal, begint met de registratie van de storing in het incidentenregistratiesysteem van I&S.
In de procedure is aangegeven dat, indien van toepassing, als nazorg een proces-verbaal door I&S op het intranet zal worden geplaatst ten behoeve van het opsporingsdossier met verwijzing naar de storing. In de procedure wordt niet aangegeven dat in geval van storing met dataverlies altijd een proces-verbaal moet worden opgesteld. In de procedure "Procedure melden van incidenten" is aangegeven dat de OVD (Officier van Dienst) verantwoordelijk is voor het opstellen van het proces-verbaal.

Voor de storing van 20 september 2012 zijn twee processen-verbaal opgemaakt door I&S. De eerste is gedateerd op 1 november 2013, waarin de bevindingen van de analyse van de historische verkeersgegevens van 20 september 2012 op één specifiek telefoonnummer met gegevens uit de actieve tap op genoemde datum zijn opgenomen. Dit proces-verbaal betreft de zaak van Van Rey en heeft betrekking op één taplijn.
Het tweede proces-verbaal is op 5 december 2013 opgemaakt voor het dataverlies van alle taps voor spraak die actief waren op 20 september 2012. Hierin wordt aangegeven dat "uit onderzoek is gebleken dat door een technisch probleem in het

1) Normstelling Inrichting Interceptiefaciliteiten, procedureel & Technisch Functioneel d.d. 31-5-2006, Communicatieprocedure naar de RICCERS bij storingen uit 2008 en Procedure melden incidenten uit 2011 en 2013.

tapsysteem op donderdag 20 september 2012 tussen 13:14 en 14:04 uur het verwerkingsproces van alle binnenkomende gesprekken is gestopt, waardoor geen verkeersgegevens en audio zijn geregistreerd. De gegevens tijdens die storing moeten als verloren worden beschouwd." Daarnaast is opgenomen dat "normaliter door de afdeling I&S direct een melding wordt gemaakt van storing met dataverlies aan de opsporing en ten spoedigste een proces-verbaal wordt opgemaakt, maar dat in dit geval dit is uitgebleven." Op dat moment zijn ook alle opsporingsteams hierover geïnformeerd.

3.2.7 *Op welke manier is de storing gelogd/geregistreerd?*

De storing is vastgelegd in (log)bestanden van het tapsysteem en niet geregistreerd in het reguliere incidentenregistratiesysteem van I&S. Registratie van de storing is wel opgenomen in de incidentenregistratiesysteem van de leverancier.

<u>Logging</u>
Op basis van analyse van de logbestanden hebben wij kunnen vaststellen dat de storing is gelogd. Het tapsysteem genereert logging over verschillende IT-componenten binnen het systeem. Voor het analyseren van de storing op 20 september 2012 zijn de volgende bestanden van belang:

1. logging op het niveau van de applicatie.
2. event-logging op het niveau van de IT-systeemcomponenten. Hierin worden veranderingen in de status van het component geregistreerd.
3. weergave van performance- en capacity issues, alsmede systeemwaarschuwingen en -fouten van hardware- en softwarecomponenten binnen het tapsysteem die naar de health-monitor worden gestuurd (als proces van monitoring en alerting).

De logging beschreven onder nummer 1 en 2 wordt veiliggesteld en was daardoor aanwezig en beschikbaar voor dit onderzoek. De informatie uit de health-monitor (nummer 3) wordt niet veiliggesteld. Na een periode van enkele weken wordt deze signaleringsinformatie overgeschreven en is daardoor niet meer aanwezig.
Op basis van de analyse van de logging nummers 1 en 2 hebben wij het verloop van de storing vastgesteld en deze komt overeen met de in paragraaf 3.2.1 aangegeven verloop. Er zijn geen logginggegevens bewaard waaruit we kunnen vaststellen dat een defecte voeding de exacte oorzaak is van de storing op 20 september 2012.

<u>Registratie</u>
In het reguliere incidentenregistratiesysteem van I&S hebben wij geen melding aangetroffen van de storing op 20 september 2012. Ook zijn geen meldingen van opsporingsteams aangetroffen waaruit zou blijken dat zij gesprekken hebben gemist.
De leverancier van het tapsysteem hanteert voor haar eigen dienstverlening een afzonderlijk registratiesysteem. Dit registratiesysteem is onafhankelijk van I&S en I&S heeft hierin geen inzicht. De leverancier heeft aangegeven dat in haar registratiesysteem twee meldingen zijn geregistreerd namelijk op 20 september 2012 om 16:03 en 16:12. Eén melding heeft de classificatie "critical", hierbij is aangeven dat sprake is geweest van dataverlies. Over de gedetailleerde informatie van deze meldingen geeft de leverancier omwille van bedrijfsgeheim geen inzage.

3.2.8 *Wat is de reden dat de geldende werkinstructie (opstellen proces-verbaal en melden storing met mogelijk dataverlies aan eindgebruikers) niet is gevolgd?*

Wij hebben geen aanwijzingen over de reden waarom de geldende werkinstructie niet is gevolgd. Een combinatie van twee factoren is mogelijk de oorzaak dat de geldende incidentenprocedure op 20 september 2012 niet is gevolgd. Deze factoren zijn: 1) de technisch beheerder van de leverancier heeft I&S niet, conform de geldende procedure, geïnformeerd over de storing; 2) op de health-monitor is deze vorm van storing mogelijk niet opgemerkt, dan wel zichtbaar geweest. Dit heeft

ertoe geleid dat I&S niet op de hoogte was van de storing en is het incidentenproces niet opgestart. Als gevolg daarvan zijn de eindgebruikers (opsporingsteams) niet geïnformeerd en is geen proces-verbaal opgesteld.

3.2.9 *Waarom is van vrijwel alle op 20 september 2012 lopende taps niet bekend hoeveel gesprekken er zijn gevoerd, terwijl de storing wel is ontdekt vóór het verstrijken van de bewaartermijn voor telecommunicatiegegevens?*

Het exact vaststellen of en hoeveel gesprekken in één tap zijn gemist door een storing, kan alleen plaatsvinden door de aanwezige verkeersgegevens van het tapsysteem te vergelijken met de historische verkeersgegevens die bij de betreffende Telecom aanbieder moeten worden opgevraagd. Om de historische verkeersgegevens op te vragen is een bevel van de Officier van Justitie nodig.

Het aantal taps op 20 september 2012 is te achterhalen uit het tapsysteem. Uit de ontvangen bestandsanalyse van registratie/log blijkt dat ongeveer 1800 taps actief waren op die dag en dat er naar verwachting ongeveer 1250 telefoongesprekken gedurende die 50 minuten zijn gevoerd. De inschatting van 1250 telefoongesprekken is gebaseerd op een vergelijking van het aantal gesprekken op de overige werkdagen in die week in september 2012 gedurende dat specifieke tijdsinterval (tussen 13:14 en 14:04 uur).

Op het moment dat de volle omvang van de storing duidelijk werd, was de wettelijke retentietermijn van 1 jaar voor het opvragen van verkeersgegevens van 20 september 2012 verstreken. Dit leiden wij af uit de volgende momenten:
1. Op 9 september 2013 komt het ontbreken van een specifiek tapgesprek in het strafdossier aan de orde.
2. De focus van het onderzoek naar het ontbrekende tapgesprek ligt op de zaak van Van Rey.
3. Op 18 september 2013 heeft I&S het vermoeden dat een storing van het tapsysteem de oorzaak moet zijn geweest van het ontbreken van het tapgesprek in de zaak Van Rey.
4. Op 19 september 2013 wordt duidelijk dat op 20 september 2012 een storing met dataverlies heeft plaatsgevonden en mogelijk ook effect had voor alle actieve taps voor spraak.
5. Op 23 september 2013 rapporteert de leverancier van het tapsysteem, op verzoek van I&S, over de toedracht en de omvang van de storing op 20 september 2012. Hieruit blijkt dat de storing betrekking had op alle actieve taps voor spraak en dat van geen van die taps in het betrokken tijdsinterval gesprekken zijn geregistreerd.

3.3 De maatregelen genomen vanaf december 2013

3.3.1 *Welke maatregelen heeft de korpschef genomen nadat de storing van 20 september 2012 in de aandacht is gekomen?*

De afspraken over de te nemen maatregelen zijn opgenomen in de brief van 17 december 2013 aan de Tweede Kamer. Deze maatregelen zijn:

1. *Het opheffen van tekortkomingen in het incidentenproces van I&S, met name:*
    a. *het aanscherpen van de instructies voor het melden van storingen van de tapmodule aan de eindgebruikers en het opstellen van het PV;*
    b. *alle storingen moeten worden geregistreerd, doorgemeld aan de eindgebruikers en adequaat en snel worden opgelost;*
    c. *indien er sprake is van dataverlies moet er altijd een PV worden opgesteld;*
    d. *het verscherpen van het toezicht op het naleven van de procedures.*

Per 11 juni 2014 is een nieuwe procesbeschrijving ‘Incidentmanagement I&S’ beschikbaar gekomen met de status definitief. De doelstelling van deze procesbeschrijving is het beter beheersen van de impact van verstoringen in het primaire proces van I&S voor teams Interceptie, zowel technisch als ook procedureel. Daarnaast is voor het stroomlijnen en beheersen van incidenten een incidentcoördinator voorzien. In aanloop op de nieuwe procesbeschrijving zijn de medewerkers en de leidinggevenden van I&S sinds december 2013 geïnstrueerd over een adequate behandeling van incidenten en is de werkwijze aangepast. Thans wordt gewerkt aan een volledige uitwerking en implementatie van het nieuwe proces.

De nieuwe procesbeschrijving voorziet in het registreren van alle (ver)storingen. Ook het informeren van de belanghebbenden over de storing en de voortgang van de oplossing is onderdeel van dit proces.
Het opdelen van het incidentenmanagementproces in fasen met de daarbij behorend procedures, voortgangsbewaking en escalatie moet zorgen voor een snelle en adequate afhandeling van storingen.

Conform het nieuwe proces van het incidentenmanagement wordt van iedere (ver)storing een impact analyse uitgevoerd. Het vaststellen dat dataverlies is opgetreden, is onderdeel van die impact analyse. In het geval dat dataverlies is opgetreden moet altijd een proces-verbaal worden opgesteld, dit is zo opgenomen in de procesbeschrijving.
Er zijn diverse oorzaken voor dataverlies. Dataverlies wordt niet alleen veroorzaakt door een storing, maar ook door een verstoring, door bijvoorbeeld een systeemupdate die moet worden doorgevoerd en een herstart met zich meebrengt. Andere oorzaken van dataverlies zijn, menselijke fouten, fouten bij de provider en technische gebreken zoals het (tijdelijk) wegvallen van een telefoongesprek. Analyse of er sprake is van dataverlies vergt de nodige capaciteit en specifieke specialismen die beperkt aanwezig is binnen de betreffende afdeling van I&S.

In het verlengde van hiervoor genoemde procesbeschrijving zijn er werkinstructies voorzien, waaronder een werkinstructie “Opmaken Proces Verbaal”. Deze werkinstructies moeten nog opgesteld worden. Van belang is dat de relatie tussen de (ver)storing en het proces-verbaal in deze werkinstructie tot uitdrukking komt.

Het aanscherpen van de instructies, registratie, opstellen proces-verbaal en verscherpen van toezicht op de naleving heeft de aandacht binnen I&S. De verwachting binnen I&S is dat eind 2014 de nieuwe procesbeschrijving, de daarbij benodigde werkinstructies en een ondersteunend incidentenregistratiesysteem zijn ingevoerd.

Uit de interviews komt verder naar voren dat de geautomatiseerde ondersteuning van het huidige incidentenregistratiesysteem niet goed aansluit op het vernieuwde incidentenmanagementproces. I&S streeft er naar om dit systeem voor het einde van 2014 aan te passen. In de tussentijd wordt gebruik gemaakt van een tijdelijke voorziening om te bewaken dat van een (ver)storing met dataverlies een proces-verbaal wordt opgesteld.

2. *De Minister heeft aangegeven in gesprek te gaan met de Korpschef over de mogelijkheden tot het treffen van een technische noodvoorziening ter voorkoming van mislukte interceptie van telefoongesprekken*

   De korpsleiding geeft aan: “Uit de analyse van de storing blijkt dat het uitbreiden van de noodvoorziening geen oplossing biedt voor het soort storingen welke leidde tot de mislukte interceptie op 20 september 2012.

De korpsleiding heeft een verkenning uitgevoerd naar de mogelijkheden tot het uitbreiden van de noodvoorziening en naar de mogelijkheden voor het verder verzwaren van het huidige systeem. De korpsleiding komt aan de hand daarvan tot de conclusie dat extra investeringen in een technische noodvoorziening afgewogen moeten worden ten opzichte van de huidige situatie. Op dit moment is sprake van een redundante opzet van het systeem waarin kritische componenten dubbel zijn uitgevoerd, een rekencentrum dat voldoet aan de wereldwijd gehanteerde eisen voor dit soort centra en hoge beschikbaarheidcijfers. Ook is voorzien in een technische noodvoorziening in de vorm van het testsysteem. Deze voorziening staat op een andere locatie dan het reguliere systeem en kan een deel van de lopende taps overnemen indien het reguliere tapsysteem volledig uit zou vallen. Daarnaast is gestart met de procedure voor vervanging van het tapsysteem in 2016. De conclusie van de korpsleiding is dan ook dat het bedrijfsmatig verstandig is om de lessen uit dit incident te vertalen in de eisen aan het nieuwe systeem en voor de bestaande situatie in te zetten op aanscherping van procedures en werkwijzen. Dit laatste is reeds in werking gesteld".

3. *De Minister heeft aangegeven om experts te laten bezien in hoeverre er mogelijkheden zijn om de technische beschikbaarheid van het tapsysteem verder te verhogen*

   De korpsleiding geeft aan: "Door experts van de landelijke eenheid en de directie Informatievoorziening is een quick scan uitgevoerd naar de mogelijkheden ter verbetering van de technische beschikbaarheid en naar de invoeringsalternatieven daarvan. Uit deze quick scan is gebleken dat verdere technische aanpassingen die het beschikbaarheidspercentage zouden kunnen verhogen boven de huidige 99,5% (beschikbaarheid zonder dataverlies als gevolg van storingen) alleen kunnen worden gerealiseerd tegen zeer hoge kosten en een grote inspanning vanuit ICT, welke ten koste zou gaan van de toch al schaarse capaciteit. Bovendien geldt voor elk technisch (complex) ICT systeem, dus ook dit tapsysteem dat een beschikbaarheid van 100% alleen in theorie mogelijk is. Tenslotte zullen deze technische aanpassingen beperkte waarde hebben totdat de geplande vernieuwing in 2016 is gerealiseerd. De mogelijkheid om de tapvoorziening op kortere termijn te vernieuwen – los van de nu getroffen maatregelen – is ook onderzocht. De huidig geplande doorlooptijd voor de vernieuwing kan niet versneld worden zonder risico's voor de continuïteit of (lopende) urgente projecten uit te stellen of te vertragen".

4. *De overdracht van het beheer van het tapsysteem van de afdeling I&S van de landelijke eenheid van de nationale politie aan de informatievoorzieningorganisatie van de nationale politie wordt versneld voorbereid*

   De korpsleiding geeft aan: "De voorbereiding is versneld voorbereid door het in kaart brengen van de risico's verbonden aan de overdracht. Dit is uitgevoerd door experts van de landelijke eenheid en de directie Informatievoorziening gezamenlijk. Deze hebben geadviseerd over de juiste aanpak en tijdsplanning. Geconstateerd is dat een versnelde overdracht van het huidige tapsysteem aan de dienst ICT risicoverhogend werkt, omdat de complexiteit van het systeem hoog is en de benodigde expertise schaars. Daarnaast speelt dat de overdracht een beroep doet op (schaarse) ICT capaciteit, hetgeen consequenties heeft voor binnen het aanvalsprogramma ICT geprioriteerde lopende of geplande projecten. Ook zullen de geformuleerde eisen aan de geplande vernieuwing in 2016 resulteren in een reductie van de afhankelijkheden tussen de diverse componenten. De korpsleiding concludeert dat op grond hiervan het logisch is de overdracht uit te voeren in samenhang met de implementatie en ingebruikname van het nieuwe systeem".

5. *Korpschef gevraagd om spoedig een voorstel te laten doen voor een nieuw stelsel voor informatiebeveiliging van de politie*

   De korpsleiding geeft aan: "Dit voorstel is afgerond en besproken in een gezamenlijke MT van politie en DGPolitie. Voor de implementatie is het nodig dat door DGPolitie oude regelgeving herzien wordt gebaseerd op het nieuwe stelsel. Onderdelen van het nieuwe stelsel voor informatiebeveiliging, zoals het beleid, het kader, de jaarplancyclus en de inrichting van de Concern Information Security Officer (CISO), zijn reeds door de korpsleiding vastgesteld en (worden) in werking gebracht.

3.3.2 In hoeverre zijn deze maatregelen op zich als voldoende te kwalificeren om een zeer hoge beschikbaarheid van het tapsysteem in de ruimste zin van het woord te garanderen? Wat is de voortgang op deze maatregelen?

In paragraaf 3.3.1 zijn de maatregelen beschreven die de Korpschef heeft getroffen nadat de storing van 20 september 2012 in de aandacht is gekomen. In deze paragraaf wordt aangegeven of deze maatregelen bijdragen aan een zeer hoge beschikbaarheid van het tapsysteem.

1) *Het opheffen van tekortkomingen in het incidentenproces van I&S*
   De aanscherping van het incidentenproces zal het optreden van storingen niet uitsluiten. Het structureel analyseren en evalueren van oorzaken van storingen vindt niet plaats. Het vergaren van kennis over de oorzaken van storingen kan bijdragen aan het garanderen van de hoge mate van de beschikbaarheid.

2) *De mogelijkheid tot het treffen van een technische noodvoorziening ter voorkoming van mislukte interceptie van telefoongesprekken*
   Een belangrijke maatregel bij een calamiteit is de mogelijkheid tot uitwijk. De bestaande uitwijkvoorziening in de vorm van het testsysteem op een andere locatie heeft niet dezelfde capaciteit als het reguliere systeem. Om deze uitwijkvoorziening effectief te laten zijn, dient te worden voorzien in een actueel uitwijkscenario en -plan. Tevens dient de uitwijkvoorziening periodiek (minimaal eenmaal per jaar) te worden getest.

3) *De minister heeft experts laten bezien in hoeverre er mogelijkheden zijn om de technische beschikbaarheid verder te verhogen*
   De werkzaamheden van deze experts (LE en IV) in het kader van de quick scan zijn beperkt gebleven tot het voeren van enkele gesprekken met het waarnemend afdelingshoofd van I&S. De rapportage over deze quick scan naar de korpsleiding heeft mondeling plaatsgevonden.
   De korpsleiding geeft aan dat, gelet op de technische beschikbaarheid zonder dataverlies van het tapsysteem 99,5% is, ervoor gekozen is te investeren in de reguliere vervanging van het tapsysteem en niet tegen hoge kosten te proberen de laatste 0,5% in het huidige systeem te reduceren.

4) *De overdracht van het beheer van het tapsysteem van de afdeling I&S aan de Dienst ICT (onderdeel IV organisatie) van de Nationale Politie wordt versneld voorbereid*
   De geformuleerde eisen aan de geplande vernieuwing van het tapsysteem in 2016, moeten de afhankelijkheden tussen de componenten van het tapsysteem reduceren. Door de reductie van de afhankelijkheden tussen de componenten van het tapsysteem is het mogelijk om het beheer van onderdelen van het tapsysteem bij dienst ICT onder te brengen. Over de relatie van deze maatregel met de hoge beschikbaarheid van het tapsysteem kunnen wij geen uitspraak doen.

5) *De Korpschef is gevraagd spoedig een voorstel te laten doen voor een nieuw stelsel voor informatiebeveiliging van de politie*.

Een adequaat stelsel voor informatiebeveiliging is randvoorwaardelijk voor een hoge beschikbaarheid. Door gerichte maatregelen kan het bijdragen aan de hoge beschikbaarheid.

3.4 De opvolging van de aanbevelingen uit eerdere reguliere audits

3.4.1 Op welke manier is opvolging gegeven aan aanbevelingen uit eerdere audits van de Auditdienst uit 2007 en 2011 en welk effect heeft dit gehad?

In deze paragraaf gaan wij in op de aanbevelingen die directe raakvlakken hebben met het omgaan van storingen in het algemeen en met de storing van 20 september 2012 in het bijzonder.

De Audits van 2007 en 2011 zijn besproken in de reguliere overleggen tussen korpschef en korpsbeheerder en hebben zij een prioritering aangebracht in de te nemen maatregelen.
Het belangrijkste advies uit de Audit van 2011 om eerst de aanbevelingen op te volgen die op het bestuurlijke / organisatorische vlak liggen is in overleg met de korpsbeheerder in 2011 overgenomen en is met het aanstellen van een voltijds security officer in 2012 grotendeels gerealiseerd. Dit is de start geweest van het verbeterproces op bestuurlijk / organisatorisch vlak.

In de rapportage over de audit uit 2011 is aangegeven dat een aantal aanbevelingen uit het onderzoek van 2007 is gerealiseerd. Dit betreft onder meer het inrichten van de testvoorziening, het gebruik van aparte logservers en het beheer van cryptografisch materiaal. De aanbevelingen die betrekking hebben op het invulling geven aan de “Normstelling Inrichting Interceptiefaciliteiten” zijn blijven staan. Deze normstelling is een ministeriele regeling en kan alleen aldaar worden aangepast.

I&S is voornemens de overige aanbevelingen mee te nemen in het totale pakket van verbeteringen van de interceptiefaciliteit. In de volgende subparagraaf worden deze toegelicht.

3.4.2 *Indien er aanbevelingen zijn waaraan onvoldoende of geen opvolging is gegeven: wat is hiervan de oorzaak?*

In eerdere audits zijn diverse aanbevelingen geformuleerd, waarvan door prioritering van de activiteiten van I&S onderstaande aanbevelingen niet ter hand zijn genomen. Deze betreffen:

1. het evalueren en actualiseren van de “Normstelling Inrichting Interceptiefaciliteit” uit 2004;
2. het opstellen van een kalender met kritieke beheershandelingen, controle op deze beheershandelingen en periodieke interne audits;
3. het treffen van maatregelen rondom leverancierstoegang tot het interceptiesysteem voor spraak.

Ad. 1. In alle auditrapportages die uitgebracht zijn over de interceptiefaciliteit is de aanbeveling gedaan om gelet op de snelheid van de technologische ontwikkelingen de normstelling op korte termijn te evalueren en deze zo nodig bij te stellen. In een brief, kenmerk 2007/12611, vraagt de toenmalige korpsleiding KLPD aan de korpsbeheerder KLPD / DG Veiligheid BZK opdracht te geven tot actualiseren de normstelling.
In het overleg tussen KorpsBeheerder (BZK, daarna VenJ) en KorpsChef (KLPD) zijn de aanbevelingen uit de auditrapportages meerdere keren aan de orde geweest. De aandacht van het overleg spitst zich toe op de aanbevelingen c.q. de maatregelen die getroffen moeten worden om de afwijkingen van de normstelling op te heffen. Wij hebben over de specifieke

aanbeveling om de normstelling te evalueren, geen concrete acties of toezeggingen aangetroffen.

Ad. 2. Voor het opstellen van een kalender met kritieke beheershandelingen moet eerst inzicht zijn in deze handelingen met de daarbij behorende risico's. I&S heeft hierin geen gestructureerd en volledig inzicht, waardoor deze activiteit is uitgebleven. In het verlengde hiervan zijn de periodieke interne audits eveneens uitgebleven.

Ad. 3. Op dit moment zijn de maatregelen voor toegang tot het tapsysteem van de technisch beheerder van de leverancier voornamelijk gericht op de fysieke en logische toegang. In het najaar 2014 is een software update voorzien, waardoor het mogelijk wordt de bevoegdheden in het tapsysteem van de technisch beheerder van de leverancier effectief in te perken.

3.5 De registratie en procedures bij storingen

3.5.1 Welke procedures gelden er wanneer een storing optreedt?

Ten tijde van de storing op 20 september 2012 waren de volgende procedures van kracht:

- De "Normstelling Inrichting Interceptiefaciliteit" uit 2004. Hierin is aangegeven aan welke voorwaarden de incidentenprocedure moet voldoen en welke aspecten van het incident moeten worden geregistreerd.
- De "Communicatieprocedure naar de RICCERS bij storingen", is een nadere uitwerking van deze normstelling en is van november 2008.
- "Procedure melden van incidenten" van augustus 2011 en augustus 2013. Dit is een aanvulling op de communicatieprocedure uit 2008.

De laatste twee procedures zijn opgegaan in de vernieuwde en uitgebreide "procesbeschrijving Incidentenmanagement I&S" die in juni 2014 formeel is vastgesteld. In aanloop hierop zijn de medewerkers en de leidinggevenden van I&S sinds december 2013 geïnstrueerd over een adequate behandeling van incidenten en is de werkwijze aangepast. Thans wordt gewerkt aan een volledige uitwerking en implementatie van het nieuwe proces.

3.5.2 Hoe is de registratie van storingen ingericht?

De wijze waarop de registratie van een technische storing plaatsvindt, is opgenomen in de procesbeschrijving Incidentenmanagement I&S, van 11 juni 2014.
Een nadere uitwerking hiervan is voorzien in de werkinstructies, waarvan de uitwerking nog moet plaatsvinden.

In deze nieuwe incidentenprocedure zijn de rollen in het proces helder aangegeven. De registratie van de meldingen is belegd bij de I&S-front office en Technisch Support. Afhankelijk van de impact van de melding wordt actie ondernomen door Techniek of door Operatie. Deze zijn tevens verantwoordelijk voor het opstellen van een proces-verbaal, indien nodig. De voortgang en afhandeling van meldingen wordt bewaakt door de incidentcoördinator van I&S.

De wijze waarop meldingen van de technisch beheerder van de leverancier van het tapsysteem worden opgenomen in de incidentenregistratie van I&S ontbreekt in deze procesbeschrijving. Hierdoor bestaat het risico dat storingen die de technisch beheerder van de leverancier waarneemt, niet geregistreerd worden in de incidentenregistratie van I&S.

In de praktijk blijkt dat de technisch beheerder van de leverancier bij technische storingen, waarbij mogelijk sprake is van dataverlies, in de regel een e-mailbericht stuurt aan medewerkers van I&S. Vervolgens registreert I&S deze melding in het

eigen incidentenregistratiesysteem. Daarnaast registreert de leverancier het incident in haar eigen registratiesysteem, voor zover deze betrekking heeft op de kwaliteit van het functioneren van haar eigen systeem.

3.5.3 *Op welke manier is de beschikbaarheid van het tapsysteem geborgd?*

In het programma van de eisen van het huidige tapsysteem zijn de volgende functionele en technische eisen opgenomen:

1) Een beschikbaarheid van 99,95%. Dit houdt in dat het systeem maximaal 263 minuten op jaarbasis niet beschikbaar mag zijn. Hierbij is het niet beschikbaar zijn van het tapsysteem als gevolg van geplande onderhoudswerkzaamheden buiten beschouwing gelaten.
2) Alle opname kritieke systemen dienen volledig redundant te zijn. Bij uitval mag geen data verloren gaan.

Daarnaast is de Normstelling inrichting interceptiefaciliteit gehanteerd voor het bepalen van de eisen voor de tapfaciliteit.

Er is een aantal maatregelen aanwezig die bijdragen aan een hoge beschikbaarheid van de tapfaciliteit. De maatregelen die in het onderzoek zijn aangetroffen, worden hieronder aangegeven. Het toetsen van deze maatregelen maakt geen deel uit van dit onderzoek.

Preventieve maatregelen: De maatregelen gericht op het voorkomen van onbeschikbaarheid zijn onder andere de dubbele uitvoering van de verwerkingscomponent, alsmede de dubbele voeding voor elk van deze verwerkingscomponenten. Ook is de opslagcomponent voorzien van een dubbele voeding.
Daarnaast is er een softwarematige overschakel voorziening tussen beide verwerkingscomponenten, die actief wordt wanneer één van beide verwerkingscomponenten uitvalt.

Detectieve maatregelen: De getroffen maatregelen om een mogelijke storing te kunnen signaleren zijn onder andere een dashboard (health-monitor) waarop medewerkers van technisch beheer de status van de componenten kunnen monitoren om mogelijke storingen adequaat te signaleren. Dit dashboard biedt de mogelijkheid om notificaties per sms te verzenden om beheerder die piketdienst hebben om hen tijdig op de hoogte te stellen van mogelijke storingen.

Repressieve maatregelen: De maatregelen die zijn getroffen om de gevolgen van eventuele onbeschikbaarheid te beperken zijn als volgt: De verwerkingscomponent beschikt over een buffer, die in het geval dat data niet kan worden weggeschreven tijdelijk de data kan vasthouden totdat de verbinding hersteld is.
Daarnaast is er een beperkte uitwijk mogelijkheid beschikbaar indien de gehele tapfaciliteit gedurende langere tijd niet beschikbaar is.

Een overstijgende maatregel is de dienstverleningsovereenkomst tussen I&S en de leverancier van het tapsysteem. I&S heeft met de leverancier van het tapsysteem de meest uitgebreide dienstverleningsovereenkomst afgesloten die de leverancier van het tapsysteem aanbiedt. Hierin is opgenomen dat er dagelijks een technisch beheerder van de leverancier on-site bij I&S aanwezig is om direct actie te ondernemen in geval van storingen.

De interne procedures van I&S zijn er op gericht om zowel de kwaliteit van de interceptie, als ook de beschikbaarheid hiervan te ondersteunen. Er zijn in deze procedures nog tekortkomingen met betrekking tot de beschikbaarheid:

- Periodiek (maandelijks) analyseren van storingen zodat bepaald kan worden welke maatregelen nodig zijn om dergelijke storingen in de toekomst te

voorkomen. Door lering te trekken uit veelvuldig voorkomende storingen, kan de beschikbaarheid worden verbeterd.
- Het uitwijk-tapsysteem heeft beperkte capaciteit. Op dit moment ontbreekt een uitwijkscenario. In dit uitwijkscenario dient ondermeer te worden aangegeven welke taps de hoogste prioriteit hebben om uit te wijken.
- Minimaal een keer per jaar dienen de uitwijkvoorziening en –scenario te worden getest om verrassingen te voorkomen, in het geval daadwerkelijk moet worden uitgeweken.

3.5.4 Welke afspraken zijn er over de beschikbaarheid dan wel het 'dienstenniveau' (service level) van het systeem?

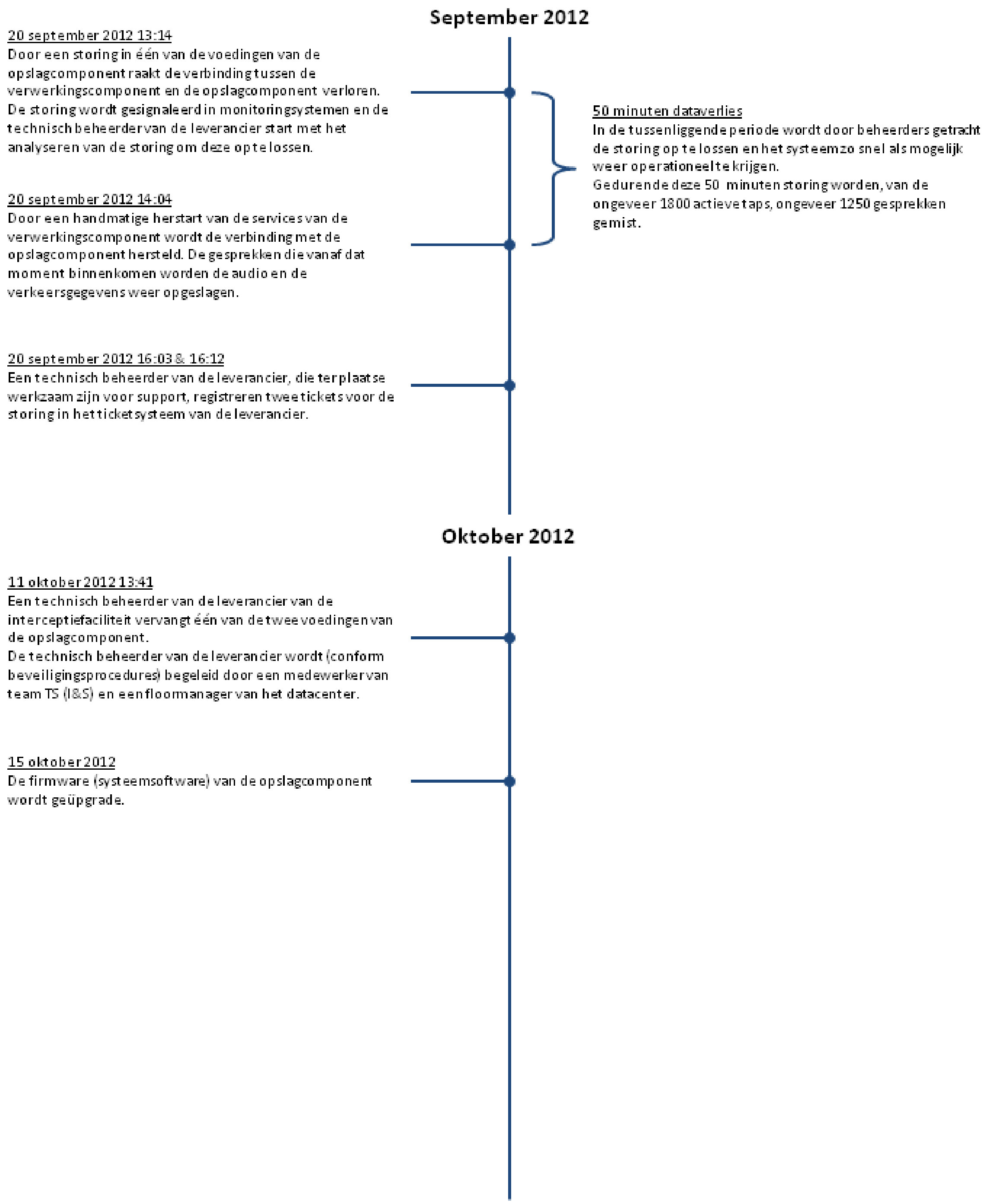
I&S en de opsporingsteams hebben afspraken gemaakt over het leveren van interceptiediensten. Deze zijn vastgelegd in een Dossier Afspraken en Procedures (DAP), een dienstverleningsovereenkomst (DVO) en een nadere overeenkomst (NOK). De relevante afspraken over de beschikbaarheid van interceptiediensten met de afnemers zijn:
- 7x24 uur bereikbaarheid van de I&S-organisatie; de beschikbaarheid van de interceptiefaciliteiten zelf is niet aangegeven.
- tijdig doorgeven aan Telecom aanbieder van een tap-aanvraag.
- spoedige uitvoering door Telecom aanbieder van de tap-aanvraag bewerkstelligen.
- invulling geven aan de normstelling inrichting interceptiefaciliteiten.
- een storings- en escalatieprocedure.

Over de beschikbaarstelling van de tapfaciliteit met de daarbij behorende serviceniveaus van I&S aan de opsporingsteams hebben wij geen concrete afspraken kunnen vinden. In de nieuwe procesbeschrijving Incidentmanagement I&S is een classificatie opgenomen van de ernst van de storing met een indicatie over de hersteltijd. Uit het document blijkt niet dat deze classificatie is afgestemd met de opsporingsteams. Ook de beschikbaarheid op jaarbasis in percentage is niet aangegeven.

Er zijn drie categorieën leveranciers van diensten en een categorie afnemers die belangrijk zijn voor de beschikbaarheid van het tapsysteem. De leveranciers zijn:
- de leveranciers van hard- en software;
- vtsPN, thans IV-organisatie, voor de netwerkverbindingen en communicatielijnen;
- de Telecom aanbieders voor het aanleveren van interceptiegegevens.

Wij hebben kennisgenomen van de overeenkomsten die met deze leveranciers zijn afgesloten. In deze overeenkomsten zijn afspraken opgenomen over de kwaliteit van de diensten, de beschikbaarheid van de dienstverlening, de wijze van het melden van (ver)storingen en de tijdigheid van het oplossen ervan.

Bijlage 1 Tijdlijnen van de storing en het incident



September 2013

9 september 2013
In een regiezitting bij de rechtbank te Rotterdam wordt door de verdediging gesteld dat het tapgesprek van 20 september 2012 ontbreekt in het dossier van het onderzoek naar dhr. van Rey.

12 september 2013
De Rijksrecherche vraagt historische verkeersgegevens in het onderzoek naar dhr. van Rey.

17 september 2013
Afdeling I&S informeert bij de Telecom aanbieder of er op 20 september 2012 een storing heeft plaatsgevonden in haar tapinfrastructuur.

18 september 2013
De Telecom aanbieder laat weten dat er op 20 september 2012 geen storing heeft plaatsgevonden in de tapinfrastructuur.

19 september 2013
Enkele medewerkers van de Landelijke Eenheid, afdeling Interceptie, worden teruggeroepen om de oorzaak van de ontbrekende gespreksopname(s) te onderzoeken. Zij komen tot de voorlopige conclusie dat dataverlies is opgetreden.

20 september 2013
De Rijksrecherche doet een 'verzoek om te bevriezen' aan de Telecom aanbieder in het onderzoek naar dhr. van Rey. Hiermee wordt verzocht om de data niet te verwijderen als gevolg van het aflopen van de retentieperiode.

20 september 2013
De Rijksrecherche vraagt wederom historische gegevens op in het onderzoek naar dhr. van Rey. Er komt geen reactie vanuit de Telecom aanbieder. Dit wordt mogelijk veroorzaakt doordat de gevraagde data reeds is verwijderd en dat de termijn van één jaar in het kader van de wet op de dataretentie is verlopen.

23 september 2013
De leverancier van het tapsysteem rapporteert, op verzoek van I&S, over de toedracht en de omvang van de storing op 20 september 2012. Hieruit blijkt dat de storing betrekking had op alle actieve taps voor spraak en dat van geen van die taps in het betrokken tijdsinterval gesprekken zijn geregistreerd.

November 2013

1 november 2013
Er wordt door I&S een proces verbaal opgesteld over het dataverlies en de ontbrekende gespreksopnames inzake het onderzoek naar dhr. van Rey.

5 november 2013
Er wordt door de Rijksrecherche een proces verbaal opgesteld over het dataverlies en de ontbrekende gespreksopnames inzake het onderzoek naar dhr. van Rey.

28 november 2013
Minister Opstelten van Veiligheid en Justitie schrijft voor de eerste maal een brief aan de tweede kamer waarin hij uitleg geeft over een storing in de voeding (stroomvoorziening) van een module van het tapsysteem van de afdeling Interceptie & Sensing.

December 2013

5 december 2013
Er wordt door I&S een proces verbaal opgesteld over het dataverlies en de ontbrekende gespreksopnames voor alle op 20 september 2012 lopende taps.

17 december 2013
Minister Opstelten informeert voor de tweede maal met een brief aan de Tweede Kamer over de storing van het tapsysteem en zegt een onafhankelijk onderzoek door de Auditdienst Rijk (ADR) toe.

Bijlage 2 Gehanteerde begrippen

In deze rapportage worden de volgende begrippen gehanteerd.

Audittrail
Een spoor van (betrouwbare) vastlegging van gegevens zodat de verwerkingsresultaten achteraf door de auditor kunnen worden gecontroleerd

Beschikbaarheid
De mate (tijdsduur) waarin een systeem gebruikt kan worden door de gebruikers voor het doel waar het systeem voor gerealiseerd is.

Cyberkey
Een cyberkey is een combinatie van een fysieke sleutel en een logische sleutel die tezamen toegang geven. De logische sleutel in de vorm van een code wordt aan de persoon uitgereikt.

Detectieve maatregelen
De maatregelen gericht om een storing te ontdekken.

Essentieel
Wezenlijk, belangrijk. Indien een essentieel onderdeel ontbreekt, werkt het geheel niet.

Firmware
Systeemsoftware die in de hardware is ingebed en waarvoor door de fabrikant van die hardware updates (verbeteringen) kunnen worden doorgevoerd.

Health-monitor
Een monitoring systeem die de status van een systeem weergeeft en bij het niet goed functioneren signalen afgeeft.

Incident
Vervelende gebeurtenis die zich voordoet dan wel in de publiciteit komt.

Informatiewaarde
De waarde die ontleend kan worden aan informatie. Bijvoorbeeld een notariële akte heeft hoge informatiewaarde.

Inspectie OOV
Inspectie Openbare Orde en Veiligheid.

Interceptiefaciliteit
De gehele interceptievoorziening die bestaat uit enkele tapsystemen (voor data en voor spraak) en uit andere onderdelen ten behoeve van ondermeer gebruik door de onderzoeksteams en centrale archivering.

Interceptie en Sensing (I&S)
Afdeling binnen de landelijke eenheid van de Nationale Politie die belast is met het beschikbaar stellen van tapfaciliteiten.

Kritiek
Kritiek moet hier worden gezien in relatie tot incident en of storing. Kritiek betekent hier dat het direct aandacht vergt voor analyse en indien nodig het treffen van maatregelen.

Logging
Het geautomatiseerd vastleggen van een bericht dat door een systeemcomponent wordt gegenereerd over een status, event of activiteit.

Online/Offline
Iets is “online” (het Engelse woord voor *aan de lijn*) wanneer het een actieve verbinding heeft met een netwerk, en “offline” wanneer dit niet zo is.

Opslagcomponent
Een onderdeel in het systeem dat bedoeld is voor de opslag van data.

Preventieve maatregelen
maatregelen die getroffen worden ter voorkomen van een storing.

Redundantie
Het meervoudig uitvoeren van een systeem of onderdelen van een systeem zodat het geheel goed blijft functioneren wanneer één of meer onderdelen defect raken of verloren gaan.

Registratie
De handmatige activiteit waarbij een interne of externe medewerker een melding van een toestand (bijv. storing) of een activiteit vastlegt in een hiervoor ingericht registratiesysteem.

Repressieve maatregelen
Maatregelen om de gevolgen van een storing te beperken.

Retentietermijn
In de Wet bewaarplicht telecommunicatiegegevens is opgenomen dat de bewaarplicht van verkeersgegevens (met betrekking tot spraak) een jaar bewaard moet worden door de Telecom aanbieder. Derhalve zijn deze gegevens na een jaar niet meer opvraagbaar.

Robuustheid
In hoeverre is het systeem toegerust om storingen op te vangen.

Server rack
Een server rack is een andere naam voor een server kast. Een server kast wordt gebruikt om verschillende hardware delen te installeren op een gemakkelijke manier. In een server kast worden dus verschillende IT componenten geplaatst.

Store and forward
Manier om informatie(pakketten) in een netwerk te verzenden, door ze tijdelijk op te slaan in tussenstations tussen begin- en eindpunt, totdat ze kunnen worden doorgestuurd naar een volgend station.

Storing
Een gebeurtenis (door technisch of menselijk falen) waardoor het systeem niet goed functioneert.

Tapsysteem
Het subsysteem (tappen van spraak, sms en levert ook verkeersgegevens) van de interceptiefaciliteit waarin de storing zich heeft voorgedaan.

Valideerbaarheid
De mate waarin de uitkomst van een berekening en/of onderzoek door een derde vastgesteld kan worden.

Verkeersgegevens
Verkeersgegevens bestaan uit de adres- en route informatie die ontstaat bij telecommunicatie. Bij telefonie zijn dat de gebelde nummers met de bijbehorende tijdstippen en de duur van elk gevoerd gesprek. De verkeersgegevens vallen glashelder te scheiden van de inhoud, het gesprek zelf.

Verstoring
Een geplande activiteit die met zich meebrengt dat het systeem een bepaalde tijd niet functioneert (bijv. het doorvoeren van wijzigingen, vervangen van hardware) en niet voor gebruik beschikbaar is.

Verwerkingscomponent
Netwerkcomponent in een telecommunicatienetwerk die gegevens ontvangt, verwerkt, omzet in een ander formaat en door zendt naar andere netwerkelementen.

vtsPN
voorziening tot samenwerking Politie Nederland. De ICT afdelingen van deze organisatie is nu de IV-organisatie van de Nationale Politie en beheert de computervloer voor de tapvoorziening.